

# Small Field Size for Secure Network Coding

Xuan Guang *Member, IEEE*, Jiyong Lu *Student Member, IEEE*, and Fang-Wei Fu

## Abstract

In network coding, information transmission often encounters wiretapping attacks. Secure network coding is introduced to prevent information from being leaked to adversaries. For secure linear network codes (SLNCs), the required field size is a very important index, because it largely determines the computational and space complexities of a SLNC, and it is also very important for the process of secure network coding from theoretical research to practical application. In this letter, we further discuss the required field size of SLNCs, and obtain a new lower bound. This bound shows that the field size of SLNCs can be reduced further, and much smaller than the known results for almost all cases.

## Index Terms

Secure network coding, field size, security-level.

## I. INTRODUCTION

In the paradigm of network coding, when wiretapping attacks occur, that is, an eavesdropper has capability of wiretapping on an unknown channel-set in networks, secure network coding is introduced to prevent information from being leaked to adversaries. This was first proposed by Cai and Yeung in [1]. In their recent paper [2], they proposed the model of a communication system on a wiretap network (CSWN) and a construction of secure linear network codes (SLNCs) to guarantee that the eavesdropper can obtain no information about the source message and meanwhile all sink nodes as legal users can decode the source message with zero error. Particularly, if the eavesdropper can obtain nothing about the source message by accessing any  $r$  channels, we say that this SLNC achieves the security-level  $r$ . Subsequently, Rouayheb *et al.* [3] showed that this model can be regarded as a network generalization

This research is supported by the National Key Basic Research Program of China (973 Program Grant No. 2013CB834204), the National Natural Science Foundation of China (Nos. 61301137, 61171082).

X. Guang is with the School of Mathematical Sciences and LPMC, J. Lu and F.-W. Fu are with the Chern Institute of Mathematics, Nankai University, Tianjin 300071, China (e-mail: xguang@nankai.edu.cn, lujiyong@mail.nankai.edu.cn, fwfu@nankai.edu.cn).

of the wiretap channel II and presented another construction of SLNCs by applying secure codes for wiretap channel II. Motivated by Rouayheb *et al.*'s formulation [3], Silva and Kschischang [4] studied the universal secure network coding via rank-metric codes, that is, the design of linear network codes for message transmission and the design of security against an eavesdropper can be completely separated from each other. For any construction of SLNCs, the required alphabet size or the size of base finite field, is very important, because it largely determines the complexities of constructions including space and computational complexities, and further efficiency of network transmission. This index is also very important for the process of secure network coding from theoretical research to practical applications. However, the existing results show that these constructions require very large field size, which leads to inefficiency in general. In [5], Feldman *et al.* derived tradeoffs between security, code alphabet, and information rate of SLNCs, which indicated that if we give up a part of overall capacity, we may use a field of smaller size. This tradeoff can be also obtained from [2] as mentioned in their paper.

Motivated by the importance of field size, in this letter, we further explore the required field size for SLNCs, and give a new lower bound. This bound shows that the field size can be reduced considerably further by applying network topologies without giving up any part of capacity. This is benefit to the implementation of SLNCs in possible applications. To be specific, by observing the constructions of SLNCs in [2]–[4], we introduce a useful equivalence relation in networks, and the number of equivalence classes induced by this equivalence relation is sufficient for the construction of SLNCs. Finally, an example is illustrated to compare our result with the previous.

## II. THE FIELD SIZE OF SLNCs

### A. Related Works

First, we state the construction proposed by Cai and Yeung [2] for designing an  $\omega$ -rate and  $r$ -security-level SLNC on a single source multicast network  $G$  with unit capacity channels. In addition, Rouayheb *et al.* [3] proposed another construction and indicated that their construction is actually equivalent to Cai and Yeung's.

#### Construction:

**Step 1:** For the information rate  $\omega$  and security-level  $r$  with  $n \triangleq \omega + r \leq C_{\min} = \min_{\text{all sinks } t} C_t$  with  $C_t$  being the minimum cut capacity between the single source  $s$  and the sink  $t$ , construct an  $n$ -dimensional  $\mathbb{F}_q$ -valued linear network code (LNC)  $\mathcal{C}_n$  of global encoding kernels  $\vec{f}_e$ ,  $e \in E$ , (e.g. Jaggi *et al.*'s algorithm [6]);

**Step 2:** Choose  $n$  linearly independent column vectors  $\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n \in \mathbb{F}_q^n$  satisfying the *secure*

condition:

$$\langle \vec{b}_i : 1 \leq i \leq \omega \rangle \cap \langle \vec{f}_e : e \in A \rangle = \{\mathbf{0}\}^1 \quad (1)$$

for all channel-subsets  $A \subseteq E$  of cardinalities no larger than  $r$ . Then define an  $n \times n$  invertible matrix  $Q = [\vec{b}_1 \ \vec{b}_2 \ \cdots \ \vec{b}_n]$ .

**Step 3:** The source message  $M$  is randomly chosen from  $\mathbb{F}_q^\omega$  and the independent random key  $K$  is distributed uniformly on  $\mathbb{F}_q^r$ , both of which are generated only at the source. Let an  $\omega$ -row vector  $\vec{m} \in \mathbb{F}_q^\omega$  and an  $r$ -row vector  $\vec{k} \in \mathbb{F}_q^r$  be the outcomes of  $M$  and  $K$ , respectively. Thus  $\vec{x} = (\vec{m}, \vec{k})$  is the input of the network, and then send the pre-encoded input  $\vec{x} \cdot Q^{-1}$  through the network by using the LNC  $\mathcal{C}_n$ .

This construction designs an  $\omega$ -rate and  $r$ -security-level SLNC. Actually,  $\{Q^{-1} \cdot \vec{f}_e : e \in E\}$  constitutes a global description of this SLNC. Evidently, the secure condition (1) must be qualified for all  $A \subseteq E$  of cardinalities no larger than  $r$  if it is qualified for those  $A \subseteq E$  with  $|A| = r$ . Hence, we just need to consider the number of channel-sets  $A$  of cardinality  $r$ , equal to  $\binom{|E|}{r}$ . Hence, we give Cai and Yeung's conclusion [2] on the required field size below.

*Theorem 1:* A  $\mathbb{F}_q$ -valued SLNC with rate  $\omega$  and security-level  $r$  can be constructed provided that  $|\mathbb{F}_q| = q \geq \binom{|E|}{r}^2$ .

### B. Our Contributions

By further observing the secure condition (1), we found that it is sufficient to consider those channel-sets  $A \subseteq E$  satisfying  $|A| = \text{Rank}(F_A) = r$  with  $F_A = [\vec{f}_e : e \in A]$ , since for any channel-set  $A' \subseteq E$  with  $|A'| = r$  but  $\text{Rank}(F_{A'}) < r$ , we can always find a channel-set  $A \subseteq E$  satisfying  $|A| = \text{Rank}(F_A) = r$  such that  $\mathcal{L}_{A'} \subset \mathcal{L}_A$ , where  $\mathcal{L}_B = \langle \vec{f}_e : e \in B \rangle$  for arbitrary channel-set  $B$ . Hence, we define a collection  $\tilde{E}_r$  consisting of all such  $A$  as:

$$\tilde{E}_r \triangleq \{A \subseteq E : |A| = \text{Rank}(F_A) = r\}.$$

The above observation implies that the required field size can be reduced to  $|\tilde{E}_r|$ . However, notice that  $\tilde{E}_r$  depends on the underlying LNC and so it is hard to handle. Naturally, we hope to find another

<sup>1</sup>Let  $L$  represent a collection of vectors in some linear space, and then we use  $\langle L \rangle$  to denote the subspace spanned by vectors in  $L$  for convenience. In addition, we always use  $\mathbf{0}$  to denote all zero column vectors throughout this letter, whose dimensions will always be clear from the context.

<sup>2</sup>Actually, as shown in [6], for the LIF algorithm, a field of size larger than or equal to  $\binom{|E|}{r}$  is sufficient for guaranteeing the existence of SLNCs.

lower bound on the field size just depending on network topologies. Thus, we define a new collection of channel-sets as:

$$\tilde{E}_r^{\text{cut}} \triangleq \{A \subseteq E : |A| = \text{mincut}(s, A) = r\}, \quad (2)$$

where  $\text{mincut}(s, A)$  represents the minimum cut capacity between  $s$  and  $A$ , and clearly  $\tilde{E}_r^{\text{cut}}$  just depends on the network topology. We first interpret some concepts just mentioned or to be used in the following. Again let  $G = (V, E)$  be a finite acyclic directed network with unit capacity channels and the single source  $s$ , and let  $A \subseteq E$  be a channel-set in  $G$ . At first, we define a cut between  $s$  and  $A$  in  $G$ . In the network  $G$ , install a new node  $t_A$ , and for every edge  $e \in A$ , add a new edge  $e'$  connected from  $\text{tail}(e)$  to the new node  $t_A$  and meanwhile delete the edge  $e$  from  $G$ . A cut between  $s$  and  $t_A$  is regarded as a cut between  $s$  and  $A$  in  $G$ , but it is necessary to mention that if a cut separating  $s$  and  $t_A$  contains some edges in  $\text{In}(t_A)$ , then they should be replaced by the corresponding edges in  $A$ . Further, the minimum cut capacity between  $s$  and  $A$  is defined as the minimum cut capacity between  $s$  and  $t_A$ , and the cuts separating  $s$  and  $A$  achieving this minimum cut capacity are called the minimum cuts. Now, we can obtain the following proposition easily, which implies that the size of  $\tilde{E}_r^{\text{cut}}$  can be regarded as a new lower bound.

*Proposition 1:*  $\tilde{E}_r \subseteq \tilde{E}_r^{\text{cut}}$ , and  $|\tilde{E}_r| \leq |\tilde{E}_r^{\text{cut}}| \leq \binom{|E|}{r}$ .

Thus, we can obtain our first conclusion.

*Theorem 2:* A  $\mathbb{F}_q$ -valued SLNC with rate  $\omega$  and security-level  $r$  can be constructed provided that  $|\mathbb{F}_q| = q \geq |\tilde{E}_r^{\text{cut}}|$ .

As we mentioned above, what we are concerned are those vector spaces spanned by global encoding kernels  $\vec{f}_e$ ,  $e \in A$ , i.e.,  $\mathcal{L}_A = \langle \vec{f}_e : e \in A \rangle$  for all  $A \in \tilde{E}_r$ , or further all  $A \in \tilde{E}_r^{\text{cut}}$ . Furthermore, notice a fact that in linear network coding, for any channel-set  $A$ , all global encoding kernels of channels in  $A$  are linear combinations of those global encoding kernels of channels in any cut CUT separating  $s$  and  $A$ . This subsequently means that  $\mathcal{L}_A$  must be a subspace of  $\mathcal{L}_{\text{CUT}}$ . Particularly, if  $A \in \tilde{E}_r^{\text{cut}}$  and CUT is a minimum cut between  $s$  and  $A$ , then  $\mathcal{L}_A \subseteq \mathcal{L}_{\text{CUT}}$ . Thus, the number of different vector spaces amongst all vector spaces  $\mathcal{L}_A$  for all  $A \in \tilde{E}_r$  or  $A \in \tilde{E}_r^{\text{cut}}$  is enough for the above Construction. Motivated by this observation, it is necessary to continue discussing the required finite field in order to reduce its size.

First, notice the following fact that  $\mathcal{L}_A = \mathcal{L}_{A'}$  for any two channel-sets  $A, A' \in \tilde{E}_r$  provided that  $A$  and  $A'$  have a common minimum cut. In addition, similar to what we indicated before, we still want to find a lower bound on the field size just depending on network topologies. Hence the following discussion is

given. At first we define a relation “ $\sim^{\text{mcut}}$ ” between arbitrary two channel-sets  $A$  and  $A'$  in  $\tilde{E}_r^{\text{cut}}$ :

$$A \sim^{\text{mcut}} A' \quad (3)$$

if and only if  $A$  and  $A'$  have a common minimum cut between the source node  $s$  and them. The theorem below shows the relation “ $\sim^{\text{mcut}}$ ” in  $\tilde{E}_r^{\text{cut}}$  being an equivalence relation.

*Theorem 3:* The relation “ $\sim^{\text{mcut}}$ ” is an equivalence relation. Equivalently, the following three properties are qualified for all channel-sets  $A, A', A'' \in \tilde{E}_r^{\text{cut}}$ :

- 1) **(Reflexivity)**  $A \sim^{\text{mcut}} A$ ;
- 2) **(Symmetry)** if  $A \sim^{\text{mcut}} A'$  then  $A' \sim^{\text{mcut}} A$ ;
- 3) **(Transitivity)** if  $A \sim^{\text{mcut}} A'$  and  $A' \sim^{\text{mcut}} A''$ ,  $A \sim^{\text{mcut}} A''$ .

The reflexivity and symmetry of the relation “ $\sim^{\text{mcut}}$ ” are obvious. To show transitivity, we need two lemmas below.

*Lemma 4:* Let  $G = (V, E)$  be a finite acyclic directed network with unit capacity channels and the single source  $s$ . Let  $t$  be a non-source node and the minimum cut capacity between  $s$  and  $t$  be  $r$ . Then arbitrary  $r$  edge-disjoint paths from  $s$  to  $t$  pass through all minimum cuts between  $s$  and  $t$ , and  $r$  distinct edges in each minimum cut are on  $r$  distinct paths respectively.

*Proof:* Assume the contrary that there exists a minimum cut CUT between  $s$  and  $t$  such that there is an edge  $e \in \text{CUT}$  on none of  $r$  paths. Note that CUT is minimum, and so  $|\text{CUT}| = \text{mincut}(s, t) = r$ , which shows that all edges in CUT are on  $r - 1$  edge-disjoint paths at most. Thus, there must exist one path passing through no edges in CUT. This further implies that after deleting all edges in CUT from the network  $G$ , there still exists a path from  $s$  to  $t$ , which conflicts with the assumption that CUT is a cut between  $s$  and  $t$ . ■

For any two edges  $e_i$  and  $e_j$  in a directed acyclic network, if a path from  $e_i$  to  $e_j$  can be found, then we say that  $e_i$  is previous to  $e_j$ , denoted by  $e_i \prec e_j$ . Particularly, we set  $e \prec e$  for every edge  $e$ . This is a natural and conventional partial order in directed acyclic networks.

*Lemma 5:* Let  $G = (V, E)$  be a finite acyclic directed network with unit capacity channels and the single source  $s$ , and let  $t$  be a non-source node of the minimum cut capacity  $r$  from  $s$ . Further let  $P_1, P_2, \dots, P_r$  be  $r$  edge-disjoint paths from  $s$  to  $t$ , and  $\text{CUT}_1 = \{e_{1,i} : 1 \leq i \leq r\}$  and  $\text{CUT}_2 = \{e_{2,i} : 1 \leq i \leq r\}$  be two minimum cuts between  $s$  and  $t$  with  $e_{j,i}$  on the path  $P_i$  for  $1 \leq i \leq r$ ,  $j = 1, 2$ .

Define an edge-set  $\text{CUT} = \{\text{minord}(e_{1,i}, e_{2,i}) : 1 \leq i \leq r\}$ , where

$$\text{minord}(e_{1,i}, e_{2,i}) = \begin{cases} e_{1,i}, & e_{1,i} \prec e_{2,i}, \\ e_{2,i}, & \text{otherwise.} \end{cases}$$

Then CUT is still a minimum cut between  $s$  and  $t$ .

*Proof:* First, since  $|\text{CUT}| = r = \text{mincut}(s, t)$ , CUT must be a minimum cut between  $s$  and  $t$  provided that it is a cut between them. Hence, we will just show that CUT is a cut between  $s$  and  $t$ . Two cases below are discussed.

**Case 1.** If  $\text{minord}(e_{1,i}, e_{2,i}) = e_{1,i}$  (resp.  $e_{2,i}$ ), i.e.,  $e_{1,i} \prec e_{2,i}$  (resp.  $e_{2,i} \prec e_{1,i}$ ) for all  $1 \leq i \leq r$ , then the result of the theorem is trivial.

**Case 2.** Otherwise, assume the contrary that CUT is no longer a cut between  $s$  and  $t$ . Then there must exist a path  $P$  from  $s$  to  $t$  which doesn't pass through CUT. But this path  $P$  has to pass through the minimum cut  $\text{CUT}_1$  from Lemma 4, and let  $e_{1,i_1}$  in  $\text{CUT}_1$  be the channel passed through by  $P$ . Then we can claim that  $e_{1,i_1} \succ e_{2,i_1}$ . Conversely, if  $e_{1,i_1} \prec e_{2,i_1}$  then  $\text{minord}(e_{1,i_1}, e_{2,i_1}) = e_{1,i_1} \in \text{CUT} \cap P$ , which leads to a contradiction. Further, we replace the part from  $e_{1,i_1}$  to  $t$  in  $P$  by the part from  $e_{1,i_1}$  to  $t$  in  $P_{i_1}$ , and keep the remaining part in  $P$ , i.e., the part from  $s$  to  $e_{1,i_1}$ , unchanged. Then we derive a new path denoted by  $P^{(1)}$ . It is easy to check that  $P^{(1)}$  doesn't pass through CUT either, since none of the parts from  $s$  to  $e_{1,i_1}$  in  $P$  and from  $e_{1,i_1}$  to  $t$  in  $P_{i_1}$  pass through CUT.

Now, we claim that the sub-path from  $s$  to  $e_{1,i_1}$  of  $P^{(1)}$  must pass through the minimum cut  $\text{CUT}_2$ . Since the part from  $e_{1,i_1}$  to  $t$  in  $P^{(1)}$  (the same as the corresponding part in  $P_{i_1}$ ) cannot pass through  $\text{CUT}_2$  from  $e_{1,i_1} \succ e_{2,i_1}$ , the path  $P^{(1)}$  would not pass through  $\text{CUT}_2$  provided that its sub-path from  $s$  to  $e_{1,i_1}$  doesn't pass through  $\text{CUT}_2$ . This contradicts to Lemma 4. Thus, assume that the sub-path from  $s$  to  $e_{1,i_1}$  of  $P^{(1)}$  passes through  $e_{2,i_2}$  in  $\text{CUT}_2$ , and similarly,  $e_{2,i_2} \succ e_{1,i_2}$ , otherwise  $\text{minord}(e_{1,i_2}, e_{2,i_2}) = e_{2,i_2} \in P^{(1)} \cap \text{CUT}$  yielding a contradiction. We further replace the part from  $e_{2,i_2}$  to  $t$  in  $P^{(1)}$  by the part from  $e_{2,i_2}$  to  $t$  in  $P_{i_2}$ , and keep the part from  $s$  to  $e_{2,i_2}$  in  $P^{(1)}$  unchanged. Then we again construct a new path  $P^{(2)}$  from  $s$  to  $t$ , which doesn't pass through CUT. Subsequently, note that the length of the sub-path from  $s$  to  $e_{2,i_2}$  of the path  $P^{(2)}$  is strictly smaller than the length of the sub-path from  $s$  to  $e_{1,i_1}$  of the path  $P^{(1)}$  because the latter covers the former and the network is acyclic.

By the same analysis as above, the path from  $s$  to  $e_{2,i_2}$  in the path  $P^{(2)}$  must pass through some channel  $e_{1,i_3}$  in  $\text{CUT}_1$  and  $e_{1,i_3} \succ e_{2,i_3}$ . Replace the part from  $e_{1,i_3}$  to  $t$  in  $P^{(2)}$  by the part from  $e_{1,i_3}$  to  $t$  in  $P_{i_3}$  and keep the part from  $s$  to  $e_{1,i_3}$  in  $P^{(2)}$  unchanged, which constitutes a new path  $P^{(3)}$  from  $s$  to  $t$  which doesn't pass through CUT. Moreover, the length of the sub-path from  $s$  to  $e_{1,i_3}$  in the path

$P^{(3)}$  is strictly smaller than the length of the sub-path from  $s$  to  $e_{2,i_2}$  in the path  $P^{(2)}$ . So far and so forth, because the length of the sub-path from  $s$  to  $e_{1,i_1}$  in the path  $P$  is finite, this process will stop at some step. This implies that finally we find a path from  $s$  to  $t$  doesn't pass through either  $\text{CUT}_1$  or  $\text{CUT}_2$ , which is a contradiction. Therefore, our hypothesis is not true, i.e.,  $\text{CUT}$  is also a cut further a minimum cut between  $s$  and  $t$ . ■

*Proof of Theorem 3:* Review the collection  $\tilde{E}_r^{\text{cut}}$  in (2) and the relation “ $\sim^{\text{mcut}}$ ” from (3). We will prove the transitivity of the relation “ $\sim^{\text{mcut}}$ ”.

First, for any  $A \in \tilde{E}_r^{\text{cut}}$ , define  $\text{MinCut}(A)$  as the collection of all minimum cuts between  $s$  and  $A$ . Let  $\text{CUT}_1$  be a common minimum cut of  $A$  and  $A'$ , i.e.,  $\text{CUT}_1 \in \text{MinCut}(A) \cap \text{MinCut}(A')$ , and similarly  $\text{CUT}_2$  be a common minimum cut of  $A'$  and  $A''$ , i.e.,  $\text{CUT}_2 \in \text{MinCut}(A') \cap \text{MinCut}(A'')$ . Further, by Menger's Theorem, we can find  $r$  edge-disjoint paths  $P_1, P_2, \dots, P_r$  from  $s$  to  $A'$ , and no other paths from  $s$  to  $A'$  exist provided deleting these  $r$  paths. Together with Lemma 4, these  $r$  paths pass through all minimum cuts in  $\text{MinCut}(A')$ , and particularly, pass through  $\text{CUT}_1$  and  $\text{CUT}_2$ . Subsequently, let  $\text{CUT}_j = \{e_{j,i} : 1 \leq i \leq r\}$ ,  $j = 1, 2$ , and let  $e_{j,i}$  be on the path  $P_i$  for all  $1 \leq i \leq r$  and  $j = 1, 2$ . Next, define a new channel-set  $\text{CUT}$ :

$$\text{CUT} = \{\text{minord}(e_{1,i}, e_{2,i}) : 1 \leq i \leq r\}^3$$

By Lemma 5, we know that  $\text{CUT}$  is still a minimum cut between  $s$  and  $A'$ , that is,  $\text{CUT} \in \text{MinCut}(A')$ . In the following, we will prove that  $\text{CUT}$  actually is a common minimum cut between  $s$  and both  $A$  and  $A''$ . In other words,  $\text{CUT} \in \text{MinCut}(A) \cap \text{MinCut}(A'')$ .

At first, we show  $\text{CUT} \in \text{MinCut}(A)$ . Conversely,  $\text{CUT} \notin \text{MinCut}(A)$ . Then there still exists a path  $P_A$  from  $s$  to  $A$  after deleting all edges in  $\text{CUT}$  from  $G$ . Subsequently, this path  $P_A$  must pass through  $\text{CUT}_1$  since  $\text{CUT}_1$  is a minimum cut between  $s$  and  $A$ . Without loss of generality, assume that  $P_A$  passes through the edge  $e_{1,1}$  in  $\text{CUT}_1$ . Then  $e_{1,1} \succ e_{2,1}$  because  $e_{1,1} \notin \text{CUT}$  and  $P_A$  doesn't pass through  $\text{CUT}$ . Furthermore, since  $\text{CUT}_1$  is also a minimum cut separating  $s$  and  $A'$ , there is a path from  $e_{1,1}$  to  $A'$ . Now, we can construct a path  $P_{A'}$  from  $s$  to  $A'$  constituted by the part from  $s$  to  $e_{1,1}$  in  $P_A$  concatenated by the part from  $e_{1,1}$  to  $A'$  in  $P_1$ . Notice none of the two parts passing through  $\text{CUT}$ . This means that  $P_{A'}$  doesn't pass through  $\text{CUT}$ , conflicting with the fact that  $\text{CUT}$  is a minimum cut separating  $s$  and  $A'$ . Thus, our hypothesis is not true and it follows  $\text{CUT} \in \text{MinCut}(A)$ .

Similarly, we can also prove  $\text{CUT} \in \text{MinCut}(A'')$ . Combining the above, we obtain  $A \sim^{\text{mcut}} A''$ . Therefore, we complete the proof of the transitivity. ■

<sup>3</sup>Actually,  $\text{CUT}$  is independent with the choice of the  $r$  paths from  $s$  to  $A'$ .

Therefore, the relation “ $\sim^{\text{mcut}}$ ” can give a partition of  $\tilde{E}_r^{\text{cut}}$  because of its equivalence property, and the number of all equivalence classes induced by “ $\sim^{\text{mcut}}$ ” forms a new lower bound on the size of the required finite field for Construction, which is our main conclusion in this letter.

*Theorem 6:* A  $\mathbb{F}_q$ -valued SLNC with rate  $\omega$  and security-level  $r$  can be constructed provided that the field size  $|\mathbb{F}_q|$  is larger than or equal to the number of equivalence classes of  $\tilde{E}_r^{\text{cut}}$  induced by the equivalence relation “ $\sim^{\text{mcut}}$ ”.

In addition, Rouayheb *et al.* [3] modified the LIF algorithm, proposed by Jaggi *et al.* [6] for constructing LNCs, to obtain a SLIF algorithm for constructing SLNCs. Although their construction is equivalent to Cai and Yeung’s in [2], their bound on the required field size of a SLNC is smaller. To be specific, for their SLIF algorithm, a SLNC with rate  $\omega$  and security-level  $r$  can be constructed over the finite field  $\mathbb{F}_q$  of size  $q \geq \binom{|E|-1}{r-1} + |T|$ , and further, combining the algorithm in [7], which uses the concept of encoding edges, with their SLIF algorithm, the corresponding field size has to satisfy  $|\mathbb{F}_q| = q \geq \binom{2C_{\min}^3|T|^2-1}{r-1} + |T|$ , which is independent to the number of channels in  $G$ . Actually, easily see that for almost all cases, our bound in Theorem 6, the number of equivalence classes, is much smaller than Rouayheb *et al.*’s two bounds. Particularly, we can also apply the algorithm in [7] to construct an auxiliary network  $\hat{G}$  from  $G$  firstly, and then apply our analysis on  $\hat{G}$ . Moreover, it is necessary to notice that the above latter bound by Rouayheb *et al.* [3] is worse than the former one in many cases. In addition, motivated by Rouayheb *et al.*’s formulation, universal secure network coding based on packet transmission is discussed in [4]. Silva and Kschischang show that this universal property can be qualified only if the packet length  $m$  must be larger than or equal to the capacity  $C_{\min}$ , and assume that the eavesdropper wiretaps  $r$  packets transmitted on  $r$  channels for every wiretap. Actually, their crucial idea is to consider the secure linear code at the source node over an extension field  $\mathbb{F}_{q^m}$ , and thus the condition (1) can be satisfied for all possible  $r \times n$  matrices  $F_A^\top$ . Hence, it is conceivable that the required field size is larger than ours. Next, we will give an example to compare our bounds with the existing results.

*Example 1:* We take the combination network  $G_1$  (see [8, p.26]) with parameters  $N = 8$  and  $k = 6$  as an example. To be specific,  $G_1$  has a single source  $s$  and  $N = 8$  internal nodes, each of which is connected from  $s$  by one and only one channel. Arbitrary  $k = 6$  internal nodes are connective with one and only one sink node, and so the number of sink nodes is  $|T| = \binom{N}{k} = \binom{8}{6} = 28$ , the number of internal nodes is  $|J| = 8$ , the number of channels is  $|E| = N + |T| \cdot k = 8 + 28 \times 6 = 176$ , and evidently the minimum cut capacity  $C_{\min}$  between  $s$  and every sink is 6. The Figure 1 is an illustration of a combination network with  $N = 3$  and  $k = 2$ .

Let the information rate and the security-level be  $\omega = 3$  and  $r = 3$ , respectively. After a simple



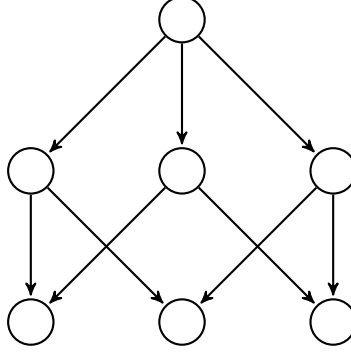


Fig. 1. Combination Network with  $N = 3, k = 2$ .

calculation, we have  $\binom{|E|}{r} = \binom{176}{3} = 893200$ . Subsequently, we analyze the cardinality of the collection  $\tilde{E}_r^{\text{cut}} = \tilde{E}_3^{\text{cut}} = \{A \subseteq E : |A| = \text{mincut}(s, A) = 3\}$ . We divide all channels in  $E$  into two layers: upper layer and lower layer. The upper layer contains all channels between  $s$  and internal nodes, and thus there are total 8 channels in this layer. The lower layer consists of all channels between internal nodes and sink nodes, and total  $|T| \cdot k = 28 \times 6 = 168$  channels in this layer. Next we will count the number of channel-sets  $A$  in  $\tilde{E}_3^{\text{cut}}$ .

- **Case1.** All three channels of  $A$  are from the upper layer. Then the number of such  $A$  in  $\tilde{E}_3^{\text{cut}}$  is  $\binom{8}{3} = 56$ .
- **Case2.** All three channels of  $A$  are from the lower layer. Notice that if three channels in the lower layer achieve capacity 3, then they have to come from different internal nodes. Together with the fact that the number of outgoing channels of every internal node is  $\binom{N-1}{k-1} = \binom{7}{5} = 21$ , the number of such  $A$  in  $\tilde{E}_3^{\text{cut}}$  is  $\binom{8}{3} \binom{21}{1} \binom{21}{1} \binom{21}{1} = 518616$ .
- **Case3.** Two channels of  $A$  are from the upper layer and the other one is from the lower layer. The number of such  $A$  in  $\tilde{E}_3^{\text{cut}}$  is  $\binom{8}{2} \binom{6}{1} \binom{21}{1} = 3528$ .
- **Case4.** Two channels of  $A$  are from the lower layer and the other one is from the upper layer. The number of such  $A$  in  $\tilde{E}_3^{\text{cut}}$  is  $\binom{8}{1} \binom{7}{2} \binom{21}{1} \binom{21}{1} = 74088$ .

Combining the above four cases, one obtains  $|\tilde{E}_3^{\text{cut}}| = 596288$ , smaller than  $\binom{|E|}{r} = 893200$ .

Next, we focus on the number of equivalence classes in  $\tilde{E}_3^{\text{cut}}$  under the relation “ $\sim^{\text{mcut}}$ ”. It is easy to deduce that any channel-set  $A$  in Cases 2, 3 and 4 must have a minimum cut in Case 1. Thus, the number of the equivalence classes is  $\binom{8}{3} = 56$ . This indicates that the required field size 56 is enough, which is much smaller than  $\binom{|E|}{r} = 893200$  and  $|\tilde{E}_r^{\text{cut}}| = 596288$ .

Further, for the two bounds on the required field size in [3], we calculate that  $\binom{|E|-1}{r-1} + |T| = 15253$

and  $\binom{2C_{\min}^3|T|^2-1}{r-1} + |T| > 5 \times 10^{10}$ . Clearly, our new bound is also much smaller than them. In addition, although the authors in [4] considered the packet network coding problem, and by contrast, we (also [2] and [3]) studied scalar network coding problem, we compare our results with theirs. It is known that the field size which can be chosen as the minimum required for multicasting is larger than or equal to the number of sink nodes, i.e.,  $|T| = 28$  here, and further the minimum cut capacity  $C_{\min}$  between  $s$  and each  $t \in T$  is 6. Thus, the field size as discussed in [4] for their universal secure scheme is at least  $28^6$ , also much larger than our result 56.

## REFERENCES

- [1] N. Cai and R. W. Yeung, "Secure network coding," IEEE Int. Symp. Inf. Theory, Lausanne, Switzerland, Jun. 30-Jul. 5, 2002.
- [2] N. Cai and R. W. Yeung, "Secure Network Coding on a Wiretap Network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424-435, Jan. 2011.
- [3] S. El Rouayheb, E. Soljanin, and A. Sprintson, "Secure Network Coding for Wiretap Networks of Type II," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1361-1371, March 2012.
- [4] D. Silva and F. R. Kschischang, "Universal secure network coding via rank-metric codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1124-1135, Feb. 2011.
- [5] J. Feldman, T. Malkin, R. A. Servedio, and C. Stein, "On the capacity of secure network coding," 42nd Ann. Allerton Conf. Commun., Contr., Comput., Monticello, IL, Sep. 29-Oct. 1, 2004.
- [6] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 1973-1982, Jun. 2005.
- [7] M. Langberg, A. Sprintson, and J. Bruck, "Network coding: A computational perspective," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 147-157, Jan. 2009.
- [8] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, "Network coding theory," *Foundations and Trends in Communications and Information Theory*, vol. 2, nos.4 and 5, pp. 241-381, 2005.